INFORMATION MANAGEMENT ELECTRONIC NEWS LETTER

"Improving Customer Awareness through better Communications"

Vol 2 Rel 11 **August 2001**

High Speed Network Future Plans; Enterprise Solution

Our ability to maintain our competitive edge will depend greatly on our ability to leverage both the corporate data that drives our business units as well as the information technology on which it travels. Whether the information we utilize comes in the form of video, voice, or data, networking technology build upon a coherent architecture that tightly couple data repositories to data users, will have a significant impact on corporate performance.

We have witnessed already the evolution of global network technologies that move data in unprecedented quantities form distributed server farms and real-time sources without loss, delay or interruption of service. The Corps of Engineers Enterprise Infrastructure Services (CEEIS) network has and continues to evolve to keep pace with our increase demands of both computer power at the regional level as well as bandwidth to move and position corporate information where it is needed to support our highly complex and robust mission needs.

The key to address existing as well as future corporate networking requirements will be determined on how well we synchronize data sources, transport infrastructure and end devices. There has been increased interest in enterprise portals (corporate portals). We have seen two types of portal emerge from the field thus far: Decision Processing Portals – evolved from data warehouses and data marts; and Collaborative portals – example Plumtree™, etc. The enterprise portal is the single gateway (internet or intranet) to relevant workflows, processes, applications systems and corporate databases on the enterprise. The network architecture and health is imperative to insure reliable and delivery of timely information.

Consider the increase use and demands of network / information technologies across the enterprise. Since enterprise information architecture (EIA) has not been effectively used for planning and design of corporate application systems many problems have arise:

- Applications design inadequacy, leading to the failure and application collapse
- Over-extended, and therefore costly, application development period
- Incompatibility of finished systems and databases with specific needs of the owener and/or end users, representing wasted effort and cost.

Senior managers are the architects of the enterprise. Strategic business planning is the approach used for enterprise architecture (EA). The CEEIS Team use of strategic plan to ensures that the enterprise address corporate requirements are met. Clear strategic plans, with an understanding by management of EA and its integration with EIA, can enable standard procedures and integrated database to be defined throughout the enterprise. From this, we can develop policies that lead to well defined quantitative goals that define what the enterprise has to achieve (Measure), by when (Time) and the degree of achievement (Level).

CEEIS as part of Department of the Army (DA) and Department of Defense (DOD), is moving out aggressively to increase our bandwidth and position the Corps networking infrastructure to support corporate mission needs. To complement this application developers / program managers need to embrace enterprise planning to leverage the networking capabilities of the CEEIS network. By doing this we can minimize the impact future applications will have on the EA by encapsulating the requirement as part of the Enterprise Information Architecture. This will insure capability and maximize interoperability across the corporate body and consistency with the EIA. More information will be provided in future newsletters as it becomes available.

Army Information Technology Regulations and Policies - A Framework From Which to Operate!

INFORMATION MANAGEMENT ELECTRONIC NEWS LETTER

"Improving Customer Awareness through better Communications"

Vol 2 Rel 11 August 2001

Evolutionary not Revolutionary: Information technology has become an essential part of our work environment for preparing, managing, and disseminating information. As technology as well as business systems evolve to address mission requirements so do the regulations and policies used to plan, acquire, and manage IT change. These regulations are not there to prevent organizations from acquiring IT resources needed to support mission requirements, but instead to insure mission needs are satisfied in the most efficient manner possible insuring that full interoperability as well as compatibility with DOD and DA IT standards are maintained.

Why do we need these regulations and policies? To start off with we have to remember that we are spending the tax payers money whenever we purchase IT not our personal money. Keeping this in mind, the regulations are there to layout a process for identifying, planning, acquiring, and sustaining IT. Without them agencies would possibly employ their own set of IT rules that may be inconsistent with strategic as well as tactical goals needed to maintain interoperability and compatibility across DOD / DA IT architecture. The regulations and policies provide agencies with a checklist to evaluate their internal IT needs, fiscal resources, and how compatible the agencies IT plans are with the rest of DOD / DA. Think of it as a blueprint for building or modifying a house. You really would have a difficult time trying to built a house and keep track of costs without a blueprint.

How do we apply the regulations and policies locally? The revised AR 25-1 Army Information Management, designates the Directorate of Information Management as the IT Program Manager for the Center, under the operational control of the Commander. The IM Director working through the Information Management Committee (IMC), plans, reviews, approves, and monitors IT initiatives for the Center. The IMC consist of all the Directors and separate Office Chiefs within the Center, who are responsible for reviewing and voting on Center-wide IT initiatives, policies, and regulations. Once approved, IM in concert with other elements of the Center, are responsible for the implementation and management of our IT programs.

I have heard of ITIPS before, how does that fit in? Another critical component of the IT planning and execution process is the Information Technology Investment Portfolio System (ITIPS) that is mandated by the Clinger-Cohen Act. ITIPS is where all of the approved IT initiatives are recorded and tracked during execution phase of the initiative. Information such as: project title, description, organization, business process identification, start up costs, as well as sustainment costs are recorded and tracked in this system. As our customers submit and record IT acquisitions into CEFMS, the ITIPS initiative control number is recorded and tracked. Here the Commander as well as management can review projected IT costs against actual costs as our IT Plan is being executed.

How does ITIPS get Updated? Annually the Center reviews its IT requirements. The information recorded in ITIPS and CEFMS form a baseline of information to plan from. Based on the review cycle, existing ITIPS initiatives will be updated and or deleted as well as new one added, which reflect what our projected strategic and operational requirements are for the out years. It should be noted that the information in ITIPS represents what our projected IT requirements are. If there is an approved initiative that needs to be added, or if the dollar amount for an existing initiative needs to be adjusted, IM is required to coordinate with our MACOM to execute this out-of-cycle requirement. The two ways which ITIPS can be updated are a result of our annual ITIPS update cycle or when required through an out of cycle submission.

So why are we doing all of this stuff? It all goes back to evaluating mission requirements, performing strategic planning, which is responsible for defining our road map for IT modernization, and programming the necessary funds to address our corporate needs. The regulations and process, when fully implemented, provides a framework for modernizing and sustaining our corporate IT infrastructure. Finally and more importantly, these regulations, policies, and related processes are required by law. They insure that government agencies properly review, document, and execute IT programs that are funded using tax payer dollars.

Potential Threats To Your PC's Security

You launch your e-mail software and see there is a message waiting for you. The subject line indicates that it is a resume for a woman named Janet Simons. You've never heard of her, but sure enough there's a Word document attached to the e-mail labeled Resume.doc. Hmm, a quick peek at it won't hurt, will it?

Think again. Opening an e-mail message, especially one with an attachment, from an unknown source is the computer equivalent of telling your kids to take candy from strangers. It is dangerous and will lead to serious trouble. Had you opened Resume.doc you could have unleashed the now-infamous Killer Resume Virus on your computer, which attempts to erase all the data on your computer, from the A: drive to the Z: drive, assuming you have that many drives attached to your system. Not only that, but if you use Microsoft's Outlook software the virus would have e-mailed itself to everyone in your address book, setting up friends, family members, colleagues, and clients for the same sort of woes.

Of course, you may want to erase all that data yourself before either crackers or unscrupulous marketing companies use their techno tricks to get their hands on it. Criminals could be poking around in your data or installing programs and viruses on your computer right now, and without the right tools, you'd never know the difference. Companies are tracking your every move on the Web, ostensibly to gather data about your habits so they can better target advertising, but also so they can sell everything from your name and address to your purchasing habits to client companies or use the information to create mailing lists. Again, this is all done transparently, and unless you know where to look and what you're looking for, there's no way to prevent it short of disconnecting your computer completely from the Internet and refusing to run software that has known security holes.

Nobody wants to be forced to take such extreme measures, so we've put together a series of articles that will tell you how to prevent security problems, as well as how to deal with disaster should it strike. What kinds of problems? How about these:

We Know Who You Are: We mentioned earlier that marketing companies are doing everything in their power to track people's Web habits, and they accomplish this with files called cookies. Before cookies came along, Web sites had no way of knowing what you were doing from one page to another. The online shopping carts that are ubiquitous today were impossible to implement because the Web site had no way of knowing that the customer had selected items on previously visited pages.

Cookies are small files that Web sites send to customers' computers so they can track what that customer has been doing at the site. If you access your Web-based e-mail account and check an option to let the browser "remember" your password so you don't have to retype it each time you access your e-mail, that password information is stored in a cookie on your computer. Whether the information is encrypted is up to the Web site that issued the cookie (and they almost universally do so when sensitive information is involved).

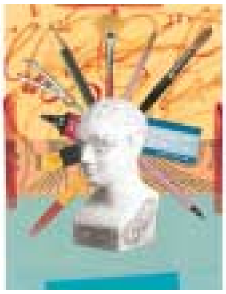
Often, cookies pose no security threat and afford a measure of convenience. In theory, the nice thing is that only the site that issued the cookie has permission to look at it. Like any technology that tracks behavior, however, cookies can be used for less-than-honorable things. As the infographic shows, Web marketing services can use special cookies to paint a frighteningly accurate portrayal of your Web activity and preferences over time.

You can manage cookies using either your browser or a third-party application, but it's harder to dupe the server logs each Web site maintains. Web sites can tell what site you were looking at before you came to their page, track how long you sit staring at any one page, and tag all of this information (and reams more) to data you've voluntarily supplied to the site, such as your age and marital status. Our advice is to never enter data into the optional information fields when you fill out Web forms, but look out for more advanced tips in the following articles that can help keep Web sites from profiling you.

The Open Invitation Of Broadband: Broadband Internet connections, such as DSL (Digital Subscriber Line) and cable modems, are increasingly popular because they offer performance and convenience benefits that dial-up modems can't approach. ISPs (Internet service providers) tout the fact that the connections are persistent, meaning they are on all the time and don't require users to connect each time they want to access the Internet. This very feature makes broadband connections more susceptible to security attacks.

When dial-up modem users finish surfing and close their Internet connections, they're immediately safe from outside attack. Granted, they can still trigger viruses already on their PCs, but broadband users face that problem and more. When they close their browsers and work with office applications or play games, their connection is still live and visible to outsiders unless some advanced security software or hardware is present. Intruders using port scanners can probe your system for weaknesses, and any open ports will be recorded as a potential weak spots for future hacking.

We know of a broadband user who received angry e-mails from other computer users telling him in no uncertain terms to stop scanning their ports, even though the broadband user wasn't running port-scanning software. It turned out an intruder had hacked into his PC, remotely installed port-scanning software, and directed that machine to probe other systems so the original intruder couldn't be traced as easily. Don't fret though, as we've said, the other articles in this section will tell you how to use firewalls and proxy servers that will keep the bad people out, and the antivirus and other internal security software that will let you rid your system of unwanted files and viruses before they can cause any damage.



Quick Tips

Ergonomics: One of the easiest ways to ward off aching wrists and arms after a day of typing at the computer is to raise the angle of the keyboard. Most keyboards include legs at their rear base that you can pop up or close, depending on your comfort preference. A few keyboards offer these legs at the front base as well so your fingers can hit the keyboard at a downward slope. Experiment to find a keyboard angle that makes your fingers and wrists most comfortable.

Microsoft Outlook: There are few things more embarrassing than sending off a mistake-ridden note to a colleague. In Microsoft Outlook 2000, click the Tools menu and select Options. Choose the Spelling tab to access the Outlook spell-check options. Under General Options, check the box next to Always Check Spelling Before Sending. You can check the boxes next to other proofreading preferences, such as whether to suggest replacements for misspelled words or not to proofread the original message in a forward or reply. When you have made your choices, click Apply, then OK.

Microsoft Word: When it's time to proofread your document and make some changes, Microsoft Word 2000 lets you compare the original version with your edited version. This lets you easily revert to the original version if you don't like what you've changed. Before you begin editing a document, open the Tools menu and scroll down to Track Changes. Now select Highlight Changes. Check the boxes next to Track Changes While Editing and Highlight Changes On Screen. Now click OK

Internet Explorer: Most Internet users have certain Web pages they like to visit regularly. We usually add these sites to our Favorites menu. But you can also easily create a Desktop shortcut to your favorite Web sites. Go to the Web site that you want to create a shortcut for and drag the icon from the upper left corner of your IE window to your Desktop. Now you can double-click the icon on your Desktop to open a browser window to that site.

Suggestions

If you would like to make a suggestion on how we can improve our services or would like to make a suggestion on ways to improve this letter please fill out our suggestion form. Click here ✉